JC685 U.S. PTO
08/28/00

JC907 U.S. PTO
09/649841
08/28/00

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1 53(b))

Attorney Docket No. 111325-000002	
First Inventor or Application Identifier: Michael C. Raley	
Title: DOCUMENT DISTRIBUTION MANAGEMENT METHOD AND APPARATUS USING A STANDARD RENDERING ENGINE AND A METHOD AND APPARATUS FOR CONTROLLING A STANDARD RENDERING ENGINE	
Express Mail Label No.	

APPLICATION ELEMENTS
See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO:
Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. [X] Fee Transmittal Form (e.g., PTO/SB/17)
   (Submit an original, and a duplicate for fee processing)
2. [X] Specification   Total Pages [24]
   (preferred arrangement set forth below)
   - Descriptive title of the Invention
   - Cross References to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to Microfiche Appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings (if filed)
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure
3. [X] Drawing(s) (35 USC 113)   Total Sheets [4]
4. [X] Oath or Declaration   Total Pages [3]
   a [X] Newly executed (original or copy)
   b [] Copy from a prior application (37 CFR 1 63(d))
      (for continuation/divisional with Box 17 completed)
      [Note Box 5 below]
      i [] DELETION OF INVENTOR(S)
         Signed statement attached deleting
         inventor(s) named in the prior application,
         see 37 CFR 1 63(d)(2) and 1 33(b).
5. [] Incorporation By Reference (useable if Box 4b is checked)
   The entire disclosure of the prior application, from which a
   copy of the oath or declaration is supplied under Box 4b,
   is considered to be part of the disclosure of the
   accompanying application and is hereby incorporated by
   reference therein

6. [] Microfiche Computer Program (Appendix)

7. [] Nucleotide and/or Amino Acid Sequence Submission
   (if applicable, all necessary)
   a [] Computer Readable Copy
   b. [] Paper Copy (identical to computer copy)
   c. [] Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. [X] Assignment Papers (cover sheet & document(s))
9. [] 37 CFR 3.73(b) Statement   [] Power of Attorney
   (when there is an assignee)
10. [] English Translation Document (if applicable)
11. [X] Information Disclosure Statement   [X] Copies of IDS
    (IDS)/PTO-1449   Citations
12. [] Preliminary Amendment
13. [X] Return Receipt Postcard (MPEP 503)
    (Should be specifically itemized)
14. [] *Small Entity   [] Statement filed in prior application,
    Statement(s)   Status still proper and desired
    (PTO/SB/09-12)
15 [] Certified Copy of Priority Document(s)
   (if foreign priority is claimed)
16. [] Other:

*A new statement is required to be entitled to pay small entity fees,
except where one has been filed in a prior application and is being
relied upon.

---

17. **If a CONTINUING APPLICATION**, check appropriate box, and supply the requisite information below and in a preliminary amendment.
[] Continuation   [] Divisional   [] Continuation-in-part (CIP)   of prior application No. _____
Prior application information: Examiner: _____   Group/Art Unit: _____

18. CORRESPONDENCE ADDRESS

[X] Customer Number or Bar Code Label   Customer No 22204   or [X] Correspondence address below

(Insert Customer No or Attach bar code label here)

Name Marc S Kaufman		
Firm. NIXON PEABODY LLP		
Address. 8180 Greensboro Drive, Suite 800		
City. McLean State VA	Zip Code. 22102	
Country: U.S.A. Telephone (703) 790-9110	FAX (703) 883-0370	

Name (Print/Type) Marc S. Kaufman	Registration No. (Attorney/Agent) 35,212
Signature	Date: August 28, 2000

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231 DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS SEND TO Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231
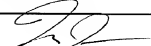
FEE TRANSMITTAL

Patent fees are subject to annual revision on October 1
These are the fees effective October 1, 1997. Small Entity
payments must be supported by a small entity statement,
otherwise large entity fees must be paid. See Forms
PTO/SB/09-12

Complete If Known

Application Number	unassigned
Filing Date	August 28, 2000
First Named Inventor	Michael C. Raley
Examiner Name	Unassigned
Group Art Unit	

TOTAL AMOUNT OF PAYMENT	730.00	Attorney Docket Number	111325-000002

METHOD OF PAYMENT (check one)

1. [X] The Commissioner is hereby authorized to charge indicated fees and
credit any over payments to:
Deposit Account No. 19-2380
Deposit Account Name: NIXON PEABODY LLP

[X] Charge Any Additional Fee Required Under 37 CFR 1.16 and 1.17
[ ] Charge the Issue Fee Set in 37 CFR 1.18 at the Mailing of the Notice of
Allowance

2. [X] Payment Enclosed:
[X] Check [ ] Money Order [ ] Other

FEE CALCULATION

1. BASIC FILING FEE

Large Entity		Small Entity			
Fee Code	Fee ($)	Fee Code	Fee ($)	Fee Description	Fee Paid
101	690	201	345	Utility filing fee	[690.00]
106	310	206	155	Design filing fee	[ ]
107	480	207	240	Plant filing fee	[ ]
108	690	208	345	Reissue filing fee	[ ]
114	150	214	75	Provisional filing fee	[ ]

SUBTOTAL (1) [$690.00]

2. EXTRA CLAIM FEES

		Extra Claims	Fee from Below	Fee Paid
Total Claims	20	- 20** = 0	X 0 =	0
Independent Claims	3	- 3** = 0	X 0 =	0
Multiple Dependent Claims			=	0

**or number previously paid, if greater, for Reissues, see below

Large Entity		Small Entity		
Fee Code	Fee ($)	Fee Code	Fee ($)	Fee Description
103	18	203	9	Claims in excess of 20
102	78	202	39	Independent claims in excess of 3
104	260	204	130	Multiple dependent claim
109	78	209	39	**Reissue independent claims over original patent
110	18	210	9	**Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) - 0 -

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity		Small Entity			
Fee Code	Fee ($)	Fee Code	Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge-late filing fee or oath	
127	50	227	25	Surcharge-late provisional filing fee or cover sheet	
139	130	139	130	Non-English specification	
147	2,520	147	2,520	For filing a request for reexamination	
112	920*	112	920*	Requesting publication of SIR prior to Examiner action	
113	1,840*	113	1,840*	Requesting publication of SIR after Examiner action	
115	110	215	55	Ext for reply within first month	
116	380	216	190	Ext for reply within second mth	
117	870	217	435	Ext for reply within third mth	
118	1,360	218	680	Ext for reply within fourth mth	
128	1,850	228	925	Ext for reply within fifth mth	
119	300	219	150	Notice of Appeal	
120	300	220	150	Filing brief in support of appeal	
121	260	221	130	Request for Oral Hearing	
138	1,510	138	1,510	Petition to institute public use proceeding	
140	110	240	55	Petition to revive-unavoidable	
141	1,210	241	605	Petition to revive-unintentional	
142	1,210	242	605	Utility issue fee (or reissue)	
143	430	243	215	Design issue fee	
144	580	244	290	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Petitions related to provisional applications	
126	240	126	240	Submission of IDS	
581	40	581	40	Recording each patent assignment per property (times number of properties)	40.00
146	690	246	345	Filing a submission after final rejection (37 CFR 1.129(a))	
149	690	249	345	For each additional invention to be examined (37 CFR 1.129(b))	
				Other	
				Other	

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) $40.00

SUBMITTED BY

Typed or Printed Name	Marc S. Kaufman
Signature	
Date	08/28/00

Complete (if applicable)

Reg. Number	35,212
Deposit Account User ID	19-2380

DOCUMENT DISTRIBUTION MANAGEMENT METHOD AND APPARATUS USING A STANDARD RENDERING ENGINE AND A METHOD AND APPARATUS FOR CONTROLLING A STANDARD RENDERING ENGINE

Field of the Invention

5   The invention relates to distribution and consumption of documents, and more particularly, to a method and apparatus for controlling various rights in, and access the content of documents displayed with the rendering engine of a standard application program, such as an Internet Web Browser.

Background of the Invention

10   The Internet is a worldwide network of computers linked together by various hardware communication links all running a standard suite of protocols known as TCP/IP (transmission control protocol/Internet protocol). The growth of the Internet over the last several years has been explosive, fueled in the most part by the widespread use of software tools (known as 15 "browsers") which allow both HTML (hypertext markup language) viewing and HTTP (hypertext transfer protocol) navigation (known as "browsers"). Browsers allow a simple GUI (graphical user interface) to be used to communicate over the Internet. Browsers generally reside on the computer used to access content on the Internet, i.e. the client computer. HTTP is a 20 component on top of TCP/IP and provides users access to documents of various formats using the standard page description language known as HTML and more recently XML (extensible markup language) and XHTML (extensible hypertext markup language), a reformulation of HTML into XML. The collection of servers on the Internet using HTML/HTTP has become 25 known as the "World Wide Web" or simply the "Web."

    Through HTML, XHTML, and interactive programming protocols, the author of content is able to make the content available to others by placing the content, in the form of a Web page, on an Internet Web server. The network path to the server is identified by a URL (Uniform Resource

Locator) and, generally, any client running a Web browser can access the Web server by using the URL. A client computer running a browser can request a display of a Web page stored on a Web server by issuing a URL request through the Internet to the Web in a known manner.

5   Since the Web utilizes standard protocols and a standard rendering engine, i.e. the rendering engine of the browser, the Web has become ubiquitous. One of the primary applications of the Web has been distribution of content in the form of documents. A "document", as the term is used herein, is any unit of information subject to distribution or transfer, including

10   but not limited to correspondence, books, magazines, journals, newspapers, other papers, software, photographs and other images, audio and video clips, and other multimedia presentations. A document may be embodied in printed form on paper, as digital data on a storage medium, or in any other known manner on a variety of media.

15   However, one of the most important issues impeding the widespread distribution of digital documents, i.e. documents in forms readable by computers, via electronic means, and the Internet in particular, is the current lack of protection of the intellectual property rights of content owners during the distribution and use of those digital documents. Efforts to resolve this

20   problem have been termed "Intellectual Property Rights Management" ("IPRM"), "Digital Property Rights Management" ("DPRM"), "Intellectual Property Management" ("IPM"), "Rights Management" ("RM"), and "Electronic Copyright Management" ("ECM"), collectively referred to as "Digital rights management (DRM)" herein. There are a number of issues in rights

25   management module: authentication, authorization, accounting, payment and financial clearing, rights specification, rights verification, rights enforcement, and document protection for example.

        In the world of printed documents, a work created by an author is usually provided to a publisher, which formats and prints numerous copies of

30   the work. The copies are then sent by a distributor to bookstores or other

retail outlets, from which the copies are purchased by end users. While the low quality of copying and the high cost of distributing printed material have served as deterrents to unauthorized copying of most printed documents, it is far too easy to copy, modify, and redistribute unprotected digital documents.

5 Accordingly, some method of protecting digital documents is necessary to make it more difficult to copy them without authorization.

Unfortunately, it has been widely recognized that it is difficult to prevent, or even deter people from making unauthorized distributions of electronic documents within current general-purpose computing and

10 communications systems such as personal computers, workstations, and other devices connected over communications networks, such as local area networks (LANs), intranets, and the Internet. Many attempts to provide hardware-based solutions to prevent unauthorized copying have proven to be unsuccessful. The proliferation of "broadband" communications technologies

15 and the development of what is presently know as the "National Information Infrastructure" (NII) will render it even more convenient to distribute large documents electronically, including video files such as full length motion pictures, and thus will remove any remaining deterrents to unauthorized distribution of documents. Accordingly, DRM technologies are becoming very

20 useful.

Two basic schemes have been employed to attempt to solve the document protection problem: secure containers and trusted systems. A "secure container" (or simply an encrypted document) offers a way to keep document contents encrypted until a set of authorization conditions are met

25 and some copyright terms are honored (e.g., payment for use). After the various conditions and terms are verified with the document provider, the document is released to the user in clear form. Commercial products such as IBM's Cryptolopes and InterTrust's Digiboxes fall into this category. Clearly, the secure container approach provides a solution to protecting the document

30 during delivery over insecure channels, but does not provide any mechanism

3

to prevent legitimate users from obtaining the clear document and then using and redistributing it in violation of content owners' intellectual property.

Cryptographic mechanisms are typically used to encrypt (or "encipher") documents that are then distributed and stored publicly, and ultimately privately deciphered by authorized users. This provides a basic form of protection during document delivery from a document distributor to an intended user over a public network, as well as during document storage on an insecure medium.

In the "trusted system" approach, the entire system is responsible for preventing unauthorized use and distribution of the document. Building a trusted system usually entails introducing new hardware such as a secure processor, secure storage and secure rendering devices. This also requires that all software applications that run on trusted systems be certified to be trusted. While building tamper-proof trusted systems is still a real challenge to existing technologies, current market trends suggest that open and untrusted systems such as PC's and workstations using browsers to access the Web, will be the dominant systems used to access copyrighted documents. In this sense, existing computing environments such as PC' s and workstations equipped with popular operating systems (e.g., Windows™, Linux™, and UNIX) and render applications such as browsers are not trusted systems and cannot be made trusted without significantly altering their architectures. Of course, alteration of the architecture defeats a primary purpose of the Web, i.e. flexibility and compatibility.

U.S. patent 5,715,403, the disclosure of which is incorporated herein by reference, discloses a system for controlling the distribution of digital documents. Each rendering device has a repository associated therewith. A predetermined set of usage transaction steps define a protocol used by the repositories for carrying out usage rights associated with a document. However, the use of repositories renders application of the system to distributed networks, such as the Internet, difficult without assuming that the

repositories are physically secure and behave in a trusted manner (which may require use of proprietary rendering engine to enforce usage rights associated with documents).

Accordingly, two basic approaches have been taken to control the distribution of documents over the Web. The first approach is the use of subscription based services in which the user is only granted access to content after paying a subscription fee. However, once the subscription fee is paid and the document is rendered by the browser, the user can copy, print, and modify the document, i.e. all control of the document by the publisher is lost.

The second approach is to utilize proprietary formats wherein the document can only be rendered by a select rendering engine that is obligated to enforce the publisher's rights. Of course, this approach requires the use of a single proprietary format and loses the ability to combine plural popular formats and the richness of content associated therewith. Further, this approach requires the user to use a previously unknown rendering application and requires development of the rendering application for each format to be rendered in a secure manner. Further, the documents must be generated or converted using non-standard tools.

Further, there are various known mechanisms by which functionality can be added to a standard rendering engine, such as a Web browser. For example, an ActiveX control can be automatically downloaded and executed by a Web browser. ActiveX is a set of rules for how applications should share information and ActiveX controls can be developed in a variety of programming languages, including C, C++, Visual Basic, and Java.

An ActiveX control is similar to a Java applet. Unlike Java applets, however, ActiveX controls have full access to the Windows™ operating system. Microsoft™ has developed a registration system so that browsers can identify and authenticate an ActiveX control before downloading it run on all

platforms, whereas ActiveX controls are currently limited to Windows environments.

A scripting language called VBScript enables Web authors to embed interactive elements in HTML documents to initiate a download and installation of ActiveX controls and other functions. Currently, Microsoft's Web browser, Internet Explorer™, supports Java, JavaScript, and ActiveX, whereas Netscape's Navigator™ browser supports only Java and JavaScript, though its plug-ins can enable support of VBScript and ActiveX.

VYOU.COM has developed a system for protecting intellectual property in documents distributed over the Web. The system includes a software plug-in, to the user's Web browser. The plug-in includes a rendering engine for the proprietary format in which documents are represented and transmitted. Accordingly, documents must be reformatted into the proprietary format and the plug-in rendering engine for the appropriate final viewing format is used in place of the standard browser rendering engine. This arrangement requires the rendering engine for each format must be developed. Therefore, this system is difficult to implement and loses the advantages of the Web as an open architecture.

The proliferation of the Web, and its usefulness in document distribution, makes it desirable to apply DRM features to Web browsers and other standard rendering engines without requiring the rendering engines to be rewritten. However, conventional DRM technologies are not easily adapted to use with Web browsers and other standard rendering engines because they require proprietary formats and rendering engines which contradict the open architecture of the Web. The inability to control application programs, such as Web browsers, independently from their rendering engines has made it difficult to apply DRM features over distribution networks.

Summary of the Invention

It is an object of the invention to facilitate distribution of digital documents.

5   It is another object of the invention to control the usage rights associated with a digital document.

It is another object of the invention to add DRM features to documents rendered with standard rendering engines.

It is another object of the invention to apply DRM technologies to an open system over a distributed network without the need for proprietary 10   formats or a plurality of proprietary rendering engines.

It is another object of the invention to minimize the need for modifying standard rendering engines when applying DRM technologies.

It is another object of the invention to facilitate compensation to authors, distributors, and other parties for publishing and distribution of digital 15   documents.

It is another object of the invention to control standard application programs independently of their associated rendering engines.

It is another object of the invention to allow the owners of content to create and distribute their content using industry standard tools and formats 20   without having to convert the content to a proprietary format.

To achieve these objects, a first aspect of the invention is a system for distributing digital documents having one or more usage rights associated therewith. The system comprises a server having at least one document stored thereon in computer readable form, a client having a standard 25   application program including a rendering engine capable of rendering unencrypted documents for viewing, a communications network coupled to the client and the server, a rights management module module for receiving a

7

request for at least one of the documents from the client and delivering the at least one document and a set of rights associated with the at least one document to the client,   a connection module adapted to be attached to the rendering engine for receiving the list of rights associated with the at least one document, a user interface module adapted to be attached to the rendering engine for controlling the access by the client to the at least one document in accordance with the set of rights associated with the at least one document.

Brief Description of the Drawing

The invention is described through a preferred embodiment and the attached drawing in which:

Fig. 1 is a block diagram of a conventional document distribution system utilizing DRM technology;

Fig. 2 is a schematic representation of a DRM system of the preferred embodiment;

Fig. 3 is a flowchart of the procedure for causing the server to respond only to a protected client in accordance with the preferred embodiment; and

Fig. 4 is a flowchart of the procedure for accessing protected content in accordance with the preferred embodiment.

Detailed Description of the Preferred Embodiment

The invention is described below with reference to a preferred embodiment. It will be apparent that the invention can be embodied in a wide variety of forms, some of which may be quite different from those of the disclosed embodiment. Consequently, the specific structural and functional details disclosed herein are merely representative and do not limit the scope of the invention.

8

Fig. 1 is a block diagram of a conventional model for a system for the electronic distribution of documents, which as defined above, may include correspondence, books, magazines, journals, newspapers, other papers, software, audio and video clips, and other files objects, and the like.

5   Author 110 creates original content 112 and passes it to a distributor 120 for distribution.   Ordinarily, author 110 is the creator of the content. However, the term "author" as used herein can be the creator, owner, editor, or other entity controlling the content or an agent (e.g. a publisher) of one of those entities. Also author 110 may distribute documents directly, without
10   involving another party as distributor 120 and thus the author and distributor may be the same entity. However, the division of functions set forth in Fig. 1 is more efficient, as it allows author 110 to concentrate on content creation and not the administrative functions of distribution.   Moreover, such a breakdown facilitates economies of scale by permitting distributor 120 to
15   associate with a number of authors 110. The term "document", as used herein, generally refers to any type of content, such as text, audio, or other data, including any encryption, formatting, or the like. The term "content", as used herein, generally refers to the underlying information of a document. However, these terms overlap and thus are used interchangeably herein.
20   Distributor 120 distributes documents to user 130 upon request. In a typical electronic distribution model, the content is distributed as a document in encrypted form. Distributor 120 encrypts the content with a random key and then encrypts the random key with a public key corresponding to user 130. Thus the encrypted document is customized solely for the particular user
25   130. User 130 is then able to use their private key to unencrypt the random key and use it to unencrypt and view the document.

Payment for the document is passed from user 130 to distributor 120 by way of clearinghouse 150 which collects requests from user 130 and from other users who wish to view a particular document. Clearinghouse 150 also
30   collects payment information, such as debit transactions, credit card transactions, or other known electronic payment schemes, and forwards the

collected payments as a payment batch to distributor 120. Of course, clearinghouse 150 may retain a share of the payment as a fee for the above-noted services. Distributor 120 may retain a portion of the batch payment from clearinghouse 150 for distribution services and forward a payment (for example royalties) to author 110. Distributor 120 may await a bundle of user requests for a single document before distributing the document. In such a case, a single encrypted document can be generated for unencryption by all of the requesting users 130.

Each time user 130 requests (or uses) a document, an accounting message is sent to audit server 140 which ensures that each request by user 130 matches with a document sent by distributor 120. Accounting information is received by audit server 140 directly from distributor 120. Any inconsistencies are transmitted via a report to clearinghouse 150, which can then adjust the payment batches made to distributor 120 accordingly. This accounting scheme is present to reduce the possibility of fraud in electronic document distribution and to handle any time-dependent usage permissions that may result in charges that vary, depending on the duration or other extent of use. The model for electronic document distribution illustrated in Fig. 1, is well known generally and can be applied to the electronic document distribution system disclosed herein.

Fig. 2 is a schematic representation of a document distribution system in accordance with a preferred embodiment of the invention. As noted above, the invention can be used in connection with known models for effecting accounting and payment of fees, such as use of a clearinghouse and an audit server. Further, the invention can be used in connection with various commerce models. Accordingly, the apparatus for auditing distribution, effecting payment, and authoring a document is not described in detail herein and is omitted from the discussion of the preferred embodiment to simplify description thereof.

As illustrated in Fig. 2, digital document distribution system 200 comprises distributor server 220, corresponding to distributor 120 described above, and client computer 230, corresponding to user 130 described above. Server 220 and client 230 can be general purpose computers programmed to

5   accomplish the desired functions. For example, server 220 can be a standard server or workstation running the Windows NT™ operating system and including HTTP server software 226 such as Apache™ or another HTTP server. Client 230 can be a personal computer running the Windows™ operating system. In the preferred embodiment, server 220 and client 230

10   are each coupled to communications network 300, such as the Internet, or more specifically, the Web. Accordingly, client 230 includes browser 232 as a standard application program having a rendering engine. Browser 232 can be any HTTP compliant browser, such as Microsoft Internet Explorer™ or Netscape Navigator™. The phrase "standard application program", as used

15   herein, refers to any application program designed to accomplish a task, such as document creation, viewing and editing, and having a rendering engine. Examples of standard application programs include word processors, Web browsers, editors, viewers, spreadsheet programs, database programs, and the like.

20   Server 220 has a plurality of documents 222 stored thereon, in the form of Web pages, for distribution. Documents 222 can be stored in an encrypted format. The term "encrypted", as used herein, refers to any mechanism by which accessibility of content is partially or completely prohibited, such as by use of asymmetric or symmetric encryption algorithms,

25   scrambling algorithms, or the like. Server 220 also includes rights management module 234, in the form of software, for storing and managing rights associated with particular ones of documents 222, users, and/or payment amounts as will be described in greater detail below.

Client 230 also has user interface (UI) module 234 and connection

30   module 236 each in the form of software and each adapted to attach to browser 232 without the need for modification of browser 232. For example,

UI module 234 and connection module 236 can be in the form of plug-ins, ActiveX controls, or in any form that allows attachment to the rendering engine of browser 232 without the need for modifying the code of browser 232. Such attachment is described in greater detail below.

5   Rights management module 224 is a server side component that identifies which rights are associated with each document 222. The rights also can vary based on the identity of the user requesting access to document 222, and/or any payment made by the user through a clearinghouse or the like. For example, the user may have the option of

10   paying one fee to view document 222 or a higher fee for viewing and printing the same document 222, as is well known. Rights management module 224 is also operative to deliver the appropriate list of rights along with the document, via communications network 300, to connection module 236 of client 230 as described below.

15   Connection module 236 is a client side software component which verifies the integrity of the environment of client 230 by verifying that UI module 234 is attached to browser 232, identifies the user of client 230, i.e. the person requesting content, retrieves the document and the appropriate list of rights sent by rights management module 224, and in appropriate

20   circumstances, unencrypts any retrieved documents that are encrypted. UI module 234 is a client side component that that monitors requests from the user to access content of documents 222 and either grants or denies the request based on the list of rights retrieved by connection module 236. Further, UI module 234 can disable specified functions of browser 232 and

25   the operating system of client 230 based on the list of rights in the manner described below, by interfacing with the operating system API and intercepting and redirecting commands for example. Connection module 236 verifies that the industry standard rendering engine running in the environment of client 230 has not been tampered with or otherwise

30   compromised in a way that may allow the user to access protected content in a way that bypasses UI module 234.

The invention can be implemented in connection with known client/server networking architectures, such as the Web, without modifying obviating, or bypassing the standard client software, server software, and rendering engines. Rights management module 224 is installed in server 220 along side the existing server software 226. As noted above, rights management module 224 identifies which rights are associated with documents 222 existing on server 220 or later stored on server 222. For example. Rights management module 224 can have a programmable database, lookup table or the like including the various rights associated with each document 222 and other variables, such as the identity of the user and the payment made by the user, in a well known manner. Rights management module 224 further interfaces with the operating system API of server 220 to cause server software 226 to only respond to connections from client(s) 230 having connection module 236 and UI module 234. In particular, once rights management module 234 is installed the procedure illustrated in Fig. 3 is accomplished. In step A, a new DRM start Web page, or other secure interface display, is created which references UI module 234 and the existing server start Web page. In step B, the various Web pages of a Web site on server 220 can be placed in a directory having a random label or any unknown directory. In step C, rights management module 224 is programmed to include a pointer to this directory and, in step D, rights management module 224 encrypts the URL of this directory. In step E, the start DRM Web page is modified to reference UI module 235 which can instruct connection module 236 to unencrypt the encrypted URL to permit access to original start page and the rest of the Web site. If client 230 does not have UI module 234 and connection module 236, the URL cannot be unencrypted and thus the Web site on server 220 cannot be accessed.

Alternatively, connection module 236 can generate a signature and send the signature to server 220 with any URL request to server 220. Access to the Web site on server 220 will only be granted if the signature is present

and valid. In this alternative, rights management module 224 can include code to validate the signature.

When a user of client computer 230 attempts to access server 220 having rights management module 224, rights management module 224 verifies if UI module 234 is installed on client 230 as described above. If not, instructions in the DRM start Web page, in the form of a java applet, ActiveX control, or the like, instruct browser 232 to download and install UI module 234. Download can be accomplished from server 220 or another server coupled to communications network 300. Such download and installation can be accomplished in a known manner using conventional mechanisms, and the user can be prompted to authorize installation and to enter other necessary information, such as where to store the installation files. Connection module 236 can be imbedded in UI module 234 and downloaded and installed simultaneously or through a separate download and installation process. Of course, if UI module 234 is detected as installed on server 230, the installation step can be skipped. If UI module 234 is not installed on client 230, and the user does not authorize such installation, access to documents on server 222 is prohibited, or limited only to documents specified as being freely distributable.

As noted above, UI module 234 and connection module 236 are in a form in which they can be attached to browser 232 without the need to modify the code of browser 232. The term "attached" as used herein with respect to the modules, refers to software modules that can be combined or coupled with browser without modifying the code of browser 232. For example, UI module 234 and connection module 236 are in the form of plug-ins, in the case of Netscape Navigator™ or ActiveX Controls in the case of Internet Explorer™. The mechanisms for developing and installing such components are well known.

The procedure for accessing protected content stored on server 220 is illustrated in Fig. 4. In step A, the DRM start Web page is accessed through

14

its URL in a known manner. In step B, the DRM start Web page directs UI module 234 to the original start page or pages referenced by the DRM start Web page using one of the methods described above. In step C, UI module 234 creates another instance of the rendering engine of browser 232, loads

5   the original start Web page, and instructs the operating system to display the new instance in a browser window, using known techniques. The new instance is directed, by UI module 234, to retrieve content from server 220 through connection module 236 in step D. In other words, in the preferred embodiment, UI module 234 intercepts commands from browser 232 and

10   redirects them through connection module 236. UI module 234 can instruct the new instance to utilize a secure asynchronous protocol through connection module 236. Therefore, UI protection is validated and all user interface events, can be intercepted and controlled in step E. For example, when the user initiates a "print" or "copy" command through the standard user

15   interface of browser 232, UI module 234 intercepts the request and only permits response if the set of rights received by connection module 236 permits the requested function to be carried out.

More specifically, when connection module 236 receives a request from the rendering engine of browser 232, connection module 236 validates

20   that the rendering engine is protected by UI module 234, i.e. UI module 234 is attached, and that the rendering engine has not been tampered with or otherwise compromised. If so, connection module 236 permits connection to rights management module 224 of server 220 and negotiates permission to retrieve the original start Web page on server 220 and the set of rights for the

25   user for the Web page. Rights management module 224 then initiates a connection between server software 226 of server 220 and connection module 236 of client 230. The connection can be established using any protocol, such as HTTP or HTTPS or any other standard or proprietary connection protocol. The requested document 222 is then retrieved and

30   delivered to connection module 236 which unencrypts document 222, if encrypted on server 220, and delivers the document in unencrypted form to

the new instance of the rendering engine of browser 232 along with the set of rights associated with the document. Once again, the contents of the set of rights may be determined based on the document, the user's identity, a payment made by the user, or any other appropriate parameter. Connection module 236 then transmits the set of rights to UI module 234 which limits the functions available to the user based on the set of rights by controlling the new instance of the rendering engine of browser 236 as described above.

The content of the document is now viewable in a window of browser 232 as any other Web page would be. However, browser 232 does not have direct access to the Web page of the document because browser 232 is "wrapped" by UI module 234. UI modules 234 prevents browser 232 from performing any prohibited functions outside of the scope of the set of rights for the document.

The invention utilizes a standard rendering engine of an application program, such as a browser, a word processor, or any other application or display program. The invention achieves this by interfacing with the application and standing between the application and the document to control access to the document. Accordingly, the invention does not require a separate proprietary rendering engine for each document format because the application rendering engine is used. Further, any data format supported by the application will be supposed by the invention without modification.

The invention can be implemented over any type of communications Network, such as the Internet, a local area network (LAN), a wide area network (WAN), direct computer connections, or the like, using any type of communication hardware and protocols. Any type of hardware or combination of hardware can be used for the various clients and servers. Accordingly, the terms "client" and "server" as used herein, can refer to any type of computing device or data terminal, such as a personal computer, a portable computer, a dumb terminal, a thin client, a hand held device, a wireless phone, or any combination of such devices. The various clients

and servers can be a single computer at a single location or multiple computers at a single or multiple locations. For example a server may be comprised of a plurality of redundant computers disposed in co-location facilities at various locations to facilitate scalability. There can be any

5   number of clients and any number of servers. The client can physically be located on the same hardware as the server.

Any appropriate server or client software can be used and any communication protocols can be used. Communication can be accomplished over electric cable, fiber optic cable, or any other cable, or in

10   a wireless manner using radio frequency, infrared, or other technologies. The various information can be stored in any format and thus the term "database" as used herein refers to any collection of information such as a database file, a lookup table, or the like. The documents can be of any type and can contain any type of content, such as text, audio information, video

15   information, or combinations of plural types of content. The portions of the invention described above that are described as software components could be implemented as hardware. Moreover, while certain functional blocks are described herein as separate and independent from each other, these functional blocks can be consolidated and performed on a single general-

20   purpose computer, or further broken down into sub-functions as recognized in the art. The set of rights can be one or more rights or rules governing use of the document, can be in any appropriate form, and can be based on various parameters such as the document type, the user's identity, a payment by the user, and the like. The various software modules can be located on the

25   client or the server.

While a preferred embodiment of the invention has been described in detail above, it should be recognized that other forms, alternatives, modifications, versions and variations of the invention are equally operative and would be apparent to those skilled in the art. The disclosure is not

30   intended to limit the invention to any particular embodiment, and is intended to embrace all such forms, alternatives, modifications, versions and

variations. Accordingly, the true scope of the invention is defined by the appended claims and legal equivalents.

What is Claimed is:

1.   A system for distributing digital documents having usage rights associated therewith, said system comprising:

a server having at least one document stored thereon in computer readable form;

5   a client having a standard application program including a rendering engine capable of rendering unencrypted documents for viewing;

a communications network coupled to said client and said server;

a rights management module module for receiving a request for at least one of the documents from said client and delivering the at least one

10   document and a set of rights associated with the at least one document to said client;

a connection module adapted to be attached to said rendering engine for receiving the list of rights associated with the at least one document;

a user interface module adapted to be attached to said rendering

15   engine for controlling access by the client to the at least one document in accordance with the set of rights associated with said at least one document.

2.   A system as recited in claim 1, wherein said connection module is operative to detect whether said user interface module is attached to said rendering engine and for providing the at least one of the documents to said

20   rendering engine if said user interface module is attached to said rendering drive.

3.   A system as recited in claim 2, wherein said connection module is operative to unencrypt the at least one of the documents.

4.   A system as recited in claim 2, wherein said standard application program is a Web browser and said server includes an HTTP server.

5.   A system as recited in claim 4, wherein said connection module and said user interface module attach to the rendering engine of the Web browser using at least one of ActiveX controls and plug-in technology.

6.   A system as recited in claim 4, wherein said rights, management module comprises means for pointing to a start Web page stored on said server, and means for encrypting said means for pointing and wherein said connection module comprises means for unencrypting said means for pointing and wherein said system further comprises means for generating a secure start Web page which references said connection module and said means for pointing.

7.   A system as recited in claim 4, wherein said connection module comprises means for generating a signature and said rights, management module comprises means for validating the signature, and wherein a request to said server is honored only if the signature is present and valid.

8.   A method for distributing digital documents having one or more usage rights associated therewith, said method comprising the steps of:

storing at least one document on a server in computer readable form;

accessing the server with a client having a standard application program including a rendering engine capable of rendering unencrypted documents;

receiving a request for at least one of the documents from the client;

delivering the at least one of the documents and a set of rights associated with the at least one of the documents to the client;

receiving the list of rights associated with the at least one of the documents with a connection module attached to the rendering engine;

controlling access by the client to the at least one of the documents in accordance with the set of rights associated with the at least one of the documents through a user interface module attached to the rendering engine.

9.   A method as recited in claim 8, further comprising the step of unencrypting the at least one of the documents.

10.   A method as recited in claim 8, further comprising the steps of detecting whether the user interface module is attached to the rendering engine and providing the at least one document to the rendering engine if the user interface module is attached to the rendering drive.

11.   A method as recited in claim 10, wherein said step of detecting further comprises determining whether said rendering engine has been compromised.

12.   A method as recited in claim 10, wherein said standard application program is a Web browser and said server includes HTTP server software.

13.   A method as recited in claim 12, further comprising the steps of providing a pointer on the server to a start Web page stored on the server, encrypting the pointer, generating a secure start Web page on the server which references the pointer, providing access to the secure start Web page through the Web browser, and unencrypting the pointer on the client to provide the Web browser access to the start Web page on the server.

14.   A method as recited in claim 12, further comprising the steps of generating a signature with the client, transmitting the signature to the server with a request to the server, validating the signature with the server, and honoring the request only if the signature is present and valid.

21

15.   In a computer architecture including a server having documents stored thereon, a start page for accessing the documents, and a client running an application program having a rendering engine, a method of distributing documents comprising the steps of:

5   installing a rights management module on the server;

attaching a user interface module and a connection module to the rendering engine;

creating a secure start page on the server;

placing the documents in directory;

10   programming the rights management module to include a pointer to the directory;

encrypting an address to the directory.

modifying the secure interface display to reference the user interface module and the start page; and

15   unencrypting the address to the directory with the connection module to permit access to the start page and the documents on the server.

16.   A method as recited in claim 15, wherein the server includes HTTP server software, wherein the application program is a Web browser, wherein the secure interface display is a secure start Web page and wherein
20   the address to the directory is in the form of a URL.

17.   A method as recited in claim 16, further comprising the steps of:

accessing the secure start Web page by issuing a URL to the start page;

directing the user interface module to the start page through the
25   reference to the start page in the secure start Web page;

22

creating an instance of the rendering engine;

loading the start page in the instance of the rendering engine to display the start page on the client;

directing the instance of the rendering engine, under control of the user interface module, to retrieve one or more of the documents from the server.

18.   A method as recited in claim 16, wherein said step of directing the instance comprises the steps of intercepting commands from the Web browser with the user interface module and redirecting the commands through the connection module on the server.

19.   A method as recited in claim 16, wherein said step of redirecting comprises the steps of instructing the instance to utilize a secure asynchronous protocol through the connection module.

20.   A method as recited in claim 16, further comprising the steps of validating, with the connection module, that the user interface module is attached to the rendering engine and permitting the client to connect to the server only if the validation step is positive.

ABSTRACT

A system and method for the secure distribution and consumption of electronic documents using a standard rendering engine. The documents have one or more usage rights associated therewith. A server stores at least one of the documents in computer readable form. A client having a standard application program including a rendering engine capable of rendering unencrypted documents for viewing is operated by a user. The client and the server are coupled by a communications network. A rights management module module receives a request for at least one of the documents on the server from the client and delivers the document and a set of rights associated with the document to the client. A connection module adapted to be attached to the rendering engine receives the set of rights associated with the document. A user interface module adapted to be attached to the rendering engine controls the user's access to the document in accordance with the list of rights for the user associated with the document.
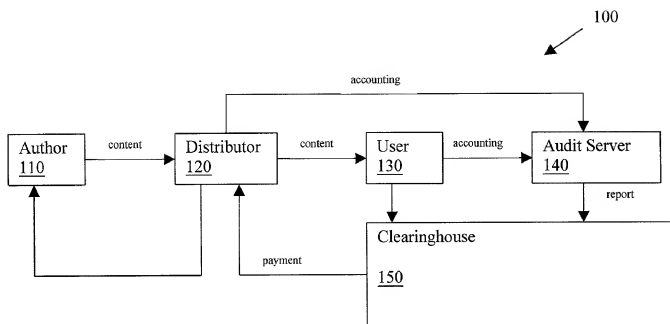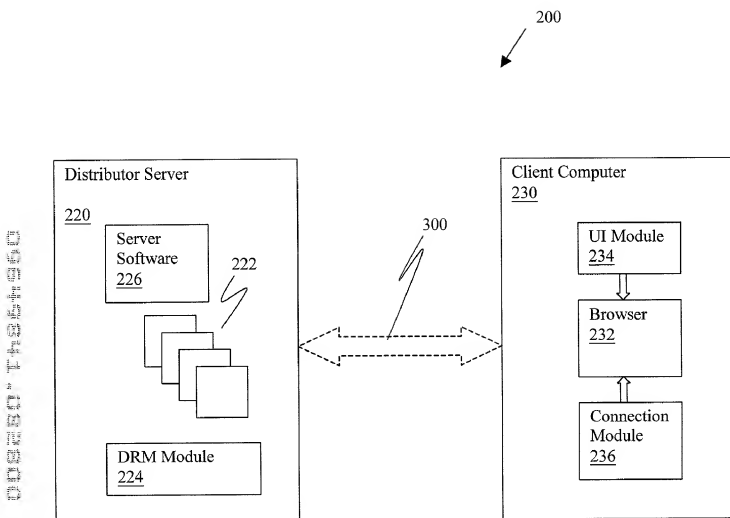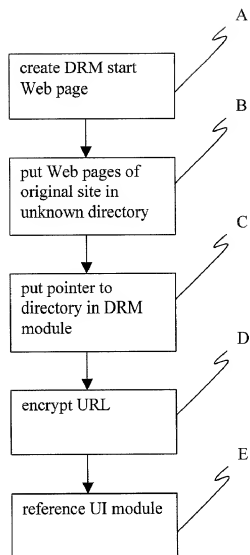
5

10

15

Fig. 1

100

Fig. 2

200

Distributor Server
220

Server
Software
226

222

DRM Module
224

300

Client Computer
230

UI Module
234

Browser
232

Connection
Module
236

create DRM start Web page — A

put Web pages of original site in unknown directory — B

put pointer to directory in DRM module — C

encrypt URL — D

reference UI module — E

Fig. 3
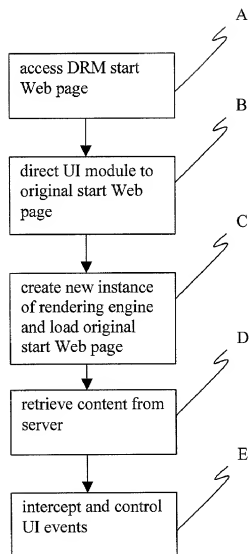
Fig. 4

DECLARATION AND POWER OF ATTORNEY   Attorney Docket No. __111325-000002__
    FOR **PATENT** APPLICATION

      As a below named inventor, I hereby declare that: my residence, post office address and citizenship are as stated next to my name; that I verily believe that I am the original, first and sole inventor (if only one name is listed below) or a joint inventor (if plural inventors are named below) of the invention entitled:
<u>DOCUMENT DISTRIBUTION MANAGEMENT METHOD AND APPARATUS USING A STANDARD
RENDERING ENGINE AND A METHOD AND APPARATUS FOR CONTROLLING A STANDARD
RENDERING ENGINE</u>_____, the specification of which
is attached hereto unless the following box is checked:

        [ ]   The specification was filed on _____
            and was assigned Serial No. _____
                             (if known)
            and was amended on _____
                             (if applicable)

    I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

    I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of federal Regulations, §1.56.

    I do not know and do not believe the same was ever known or used in the United States of America before my or our invention thereof, or patented or described in any printed publication in any country before my or our invention thereof, or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months prior to this application, and that no application for patent or inventor's certificate on this invention has been filed in any country foreign to the United States of America prior to this application by me or my legal representatives or assigns, except as follows:

    I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and checked at right:

Prior Foreign Application(s) (Number) (Month/Day/Year Filed)	(Country)	Priority Claimed	
		Yes	No

All foreign applications, if any, for any Patent or Inventor's Certificate filed more than 12 months prior to the filing date of this application:

Country	Application No.	Date of Filing (Month/Day/Year)

I hereby claim the benefit under Title 35, United States Code, §119(e) or §120, as applicable, of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Application Serial No.	Filing Date	Status: patented, pending, abandoned

I hereby appoint the following attorneys to prosecute this application and/or any international application and to transact all business in the Patent and Trademark Office connected therewith:

Daniel W. Sixbey, (Reg. No. 20,932)
Charles M. Leedom, Jr. (Reg. No. 26,477)
Thomas W. Cole (Reg. No. 28,290)
Donald R. Studebaker (Reg. No. 32,815)
Tim L. Brackett (Reg. No. 36,092)
Robert M. Schulman (Reg. No. 31,196)
Marc S. Kaufman (Reg. No. 35,212)
William J. Healey (Reg. No. 36,160)
Kenneth H. Salen (Reg. No. 43,077)
James E. Howard (Reg. No. 39,715)

Stuart J. Friedman (Reg. No. 24,312)
David S. Safran (Reg. No. 27,997)
Joan K. Lawrence (Reg. No. 29,940)
Jeffrey L. Costellia (Reg. No. 35,483)
Eric J. Robinson (Reg. No. 38,285)
Daniel S. Song (Reg. No. 43,143)
Corinne R. Gorski (Reg. No. 34,339)
Brian C. Oakes (Reg. No. 41,467)
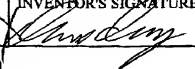Jason H. Vick (Reg. No. 45,285)

Send Correspondence to: _____

NIXON PEABODY LLP
8180 Greensboro Drive, Suite 800
McLean, Virginia 22102
Telephone: (703) 790-9110

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both,

under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

The undersigned hereby authorize any U.S. attorney or agent named herein to accept and follow instructions from _____ as to any action to be taken in the Patent and Trademark Office regarding this application without direct communication between the U.S. attorney or agent and the undersigned. In the event of a change in the persons from whom instructions may be taken, the U.S. attorneys or agents named herein will be so notified by the undersigned.

FULL NAME OF SOLE OR FIRST INVENTOR Michael Charles Raley	INVENTOR'S SIGNATURE	DATE 2-28-00
RESIDENCE (City, State & Country) Downey, California , United States of America		CITIZENSHIP USA
POST OFFICE ADDRESS (Complete Address including City, State & Country) 12834 Verdura Avenue, Downey, CA 90242 USA		